Fiche réflexe

Compromission d'un compte de messagerie

Endiguement

2025

Présentation de la fiche

1 A qui s'adresse-t-elle ?

- Responsables de la sécurité des systèmes d'information (RSSI)
- Administrateurs du système d'information

2 Quand l'utiliser ?

Utiliser cette fiche lorsqu'une **compromission est suspectée ou confirmée sur un compte de messagerie**.

3 A quoi sert-elle ?

L'objectif de cette fiche est de proposer les premières actions **d'endiguement** ayant pour objectif de circonscrire l'attaque. Elles tenteront de **limiter son extension et son impact** et de donner du temps de s'organiser à la défense et de reprendre l'initiative.

4 Comment l'utiliser ?

Deux parties principales composent cette fiche :

- La partie **Actions d'endiguement par priorités** pointe l'ordre prioritaire des actions détaillées dans la partie suivante.
- La partie **Actions d'endiguement par thèmes** détaille les différentes actions d'endiguement possibles selon 4 axes thématiques.

Si l'organisation estime avoir besoin d'aide pour réaliser ces actions d'endiguement, elle peut contacter des équipes spécialisées en réponse à incident, qu'elles soient internes ou externes : voir la partie **Contacts**.

Sommaire

Fiche réflexe
- Compromission d'un compte de messagerie – Endiguement

Prérequis

01

Avoir qualifié l'incident

Avoir **qualifié** que l'incident en cours sur mon système d'information est bien une **compromission d'un compte de messagerie** et en avoir évalué la gravité :

Fiche précédente conseillée : Fiche réflexe - Compromission d'un compte de messagerie – Qualification

Les mesures d'endiguement proposées dans cette fiche devront être appliquées en cohérence avec les conclusions de la **qualification** : le **périmètre** affecté par l'incident, son **impact** potentiel sur l'organisation, **l'urgence** à résoudre la situation, etc.

02

Avoir les capacités d'administration

S'assurer que les personnes qui mettront en œuvre les actions d'endiguement ont les **droits d'accès** au système d'administration de la messagerie, l'accès aux comptes affectés, si possible avec les personnes qui en sont victimes, et les accès aux journaux des solutions liées à la messagerie.

Si le système d'information est infogéré, s'assurer de la capacité à mobiliser l'infogérant dans l'urgence.

03

Ouvrir une main courante*

Dès le début de l'incident, ouvrir une **main courante** pour **tracer toutes les actions et événements** survenus sur le système d'information dans un **ordre chronologique**. Chaque ligne de ce document doit représenter une action avec au minimum trois informations :

1. La date et l'heure de l'action ou de l'évènement (si estimé nécessaire, ajouter le fuseau horaire UTC) ;
2. Le nom de la personne ayant réalisé cette action ou ayant informé sur l'évènement ;
3. La description de l'action ou de l'évènement et les machines concernées.

Ce document sera utile pour :

- Réaliser un historique du traitement de l'incident et partager la connaissance ;
- Piloter la coordination des actions et suivre leur état d'avancement ;
- Évaluer l'efficacité des actions et leurs potentiels impacts non prévus.

*Cette main courante doit être **éditable et consultable** par tous les intervenants. Il est déconseillé de la stocker sur le système d'information compromis, où elle serait accessible par l'attaquant. En revanche, cette main courante peut être accessible sur un partage de fichiers en ligne (cloud) ou intégrée dans le logiciel de gestion d'incident ou le SIEM si l'organisation en possède un, voire être au format papier.

Actions d'endiguement par priorités

Cette partie présente l'ordre prioritaire des actions détaillées dans la partie suivante :

Actions	Priorité
Déclarer l'incident	P0
Reprendre le contrôle du compte compromis (Mesure 1)	P0
Nettoyer les emprises restantes sur le compte compromis (Mesure 2)	P0
Protéger le poste de l'utilisateur compromis (Mesure 3)	P1
Protéger les autres accès de l'utilisateur compromis au SI de l'organisation (Mesure 4)	P1
Préserver les traces (Mesure 9)	P2
Limiter la propagation depuis la messagerie compromise (Mesure 6)	P2
Entraver l'attaquant (Mesure 7)	P2
Investiguer le système d'information (Mesure 8)	P3
Sécuriser la solution de messagerie (Mesure 3)	P4
Sensibiliser l'utilisateur (mesure 10)	P4

Actions d'endiguement par thèmes

Déclarer l'incident

Obligation de déclarer les incidents au CERT Santé

En vertu de l'article L1111-8-2 du Code de la santé publique, les établissements de santé, les laboratoires de biologie médicale, les centres de radiothérapie et les établissements et services médico-sociaux sont tenus de **signaler tout incident de sécurité des systèmes d'information aux autorités compétentes**.

Contacts du CERT Santé

- **Numéro d'urgence 24h/24 et 7j/7** : 09 72 43 91 25
- **Contact mail** : cyberveille@esante.gouv.fr
- **Portail de signalement** : https://signalement.social-sante.gouv.fr/espace-declaration/profil

Procédure pour déclarer un incident

1) Accéder au portail de signalement : https://signalement.social-sante.gouv.fr/espace-declaration/profil
2) Cliquer sur "**Je suis un professionnel de santé**"
3) Sélectionner "**Cybersécurité**" dans la liste
4) Cocher la case "**Incident de sécurité des systèmes d'information**"
5) Réaliser la procédure pour déclarer l'incident

Actions d'endiguement par thèmes

Une compromission d'un compte de messagerie indique qu'il y a eu une action malveillante sur le compte en question, mais l'incident a pu s'étendre à d'autres comptes ou systèmes. La remédiation ne doit donc pas être limitée à un simple changement de mot de passe, mais doit faire l'objet de mesures complémentaires pour limiter l'extension de la compromission.

Lors d'une compromission d'un compte de messagerie, il peut être complexe de déterminer l'ampleur de l'incident qui en a résulté. Il peut être limité à de l'espionnage et de l'exfiltration de données du compte compromis, mais également servir d'accès initial pour attaquer d'autres comptes, réaliser des escroqueries comme l'arnaque au président, attaquer des systèmes, etc.

Cette partie détaille les différentes mesures d'endiguement possibles selon 6 axes thématiques. Chaque **mesure** est ensuite scindée en **actions unitaires** :

- **Protéger la messagerie**
  - Mesure 1 - Reprendre le contrôle du compte compromis
  - Mesure 2 - Nettoyer les emprises restantes sur le compte compromis
- **Protéger l'environnement de l'utilisateur compromis**
  - Mesure 3 - Protéger les autres accès à l'organisation de l'utilisateur compromis
  - Mesure 4 - Protéger le poste de l'utilisateur compromis
- **Préparer l'investigation**
  - Mesure 5 - Préserver les traces
- **Limiter l'extension de la compromission**
  - Mesure 6 - Limiter la propagation depuis la messagerie compromise
  - Mesure 7 - Entraver l'attaquant
- **Débuter l'investigation**
  - Mesure 8 - Investiguer le système d'information
- **Sécuriser l'organisation**
  - Mesure 9 - Sécuriser la solution de messagerie
  - Mesure 10 - Sensibiliser l'utilisateur

Les actions présentées dans cette partie sont regroupées par thèmes, et non par priorités ! Pour cela, se référer à la partie précédente *Actions d'endiguement par priorités*.

Actions d'endiguement par thèmes

Protéger la messagerie

Mesure 1 - Reprendre le contrôle du compte compromis

Pour tout compte de messagerie compromis, les identifiants doivent être réinitialisés et les emprises nettoyées, afin de supprimer les accès illégitimes de l'attaquant :

Action 1.a : Bloquer le compte de messagerie

❑ Bloquer le compte, si possible, en attendant une levée de doute avec l'utilisateur victime
❑ Ne débloquer le compte qu'au moment de sa réinitialisation

Impacts : Selon les solutions de messagerie, cette action peut empêcher de recevoir des courriels et avoir des impacts sur l'utilisation d'autres services accédés par le compte.

Action 1.b : Réinitialiser le compte de messagerie compromis

❑ Révoquer les sessions actives/tokens du compte
❑ Forcer la réinitialisation du **mot de passe** du compte
❑ Si le compte utilise un **MFA**, forcer son réenregistrement
  - Si non encore utilisé, activer le **MFA** en mode **Enforce** (et non juste en mode Audit)

Action 1.c : Nettoyer les persistances et accès illégitimes sur le compte compromis

❑ Supprimer les **MFA** illégitimement ajoutés au compte
❑ Supprimer les accès des appareils suspects pouvant accéder à la messagerie sans MFA

Actions d'endiguement par thèmes

Protéger la messagerie

Mesure 2 - Nettoyer les emprises restantes sur le compte compromis

Action 2.a : Nettoyer les règles de gestion sur le compte compromis

- ❑ Supprimer les **délégations** illégitimes sur la boîte aux lettres du compte
- ❑ Désactiver les règles de **transfert automatique** à un compte tiers
- ❑ Désactiver d'autres règles de gestion qui sembleraient illégitimes (permissions, etc.)

Action 2.b : Nettoyer les accès d'applications tierces au compte compromis

- ❑ Détecter un accès frauduleux via une extension logicielle (plugin) ou une application tierce

Action 2.c : Nettoyer les actions d'administration illégitimes

Si le compte avait des droits d'administration, investiguer les journaux et nettoyer ses actions illégitimes :

- ❑ Supprimer les comptes utilisateurs illégitimement créés
- ❑ Supprimer les privilèges suspects ajoutés à d'autres comptes utilisateurs, puis effectuer une levée de doutes sur ces comptes

Actions d'endiguement par thèmes

Protéger l'environnement de l'utilisateur compromis

Mesure 3 - Protéger le poste de l'utilisateur compromis

Action 3.a : Protéger le poste utilisateur

- ❑ Surveillez de potentielles notifications antivirales sur le poste
- ❑ Si des éléments vous amènent à soupçonner une compromission du poste (hameçonnage, vol d'identifiants, etc.), vous pouvez basculer sur la procédure adéquate
- ❑ Dans le doute, faire une analyse antivirale complète du poste ou le réinstaller

Mesure 4 - Protéger les autres accès à l'organisation de l'utilisateur compromis

Action 4.a : Réinitialiser les accès de l'utilisateur aux autres applications de l'organisation

- ❑ Forcer la réinitialisation des **mots de passe** de tous les comptes de l'organisation associés à la victime, en priorité des applications accessibles depuis Internet
- ❑ Révoquer les **sessions actives/tokens** de tous les comptes de l'organisation associés à la victime, en priorité des applications accessibles depuis Internet
    - Ne pas oublier le VPN, les autres accès à distance et services cloud

Important :
Un *phishing* ou autre vol de données n'a pu extraire qu'un seul couple login/mot de passe, mais qui peuvent potentiellement être réutilisables sur d'autres applications.
Un *info stealer* a pu extraire du navigateur de l'utilisateur compromis non seulement plusieurs couples login/mot de passe, mais également des tokens de sessions actives.

Actions d'endiguement par thèmes

Préparer l'investigation

Mesure 5 - Préserver les traces

Action 5.a : Augmenter la verbosité et la rétention des journaux

- ❑ Il convient d'augmenter autant que possible la verbosité et la rétention des données sur les comptes compromis
- ❑ Il est également possible de demander l'augmentation des journaux disponibles au fournisseur de la solution de messagerie, selon son contrat

Action 5.b : Préserver les journaux du compte compromis

- ❑ Exporter les journaux, si possible centrés sur le compte compromis, pour ne pas supprimer des traces utiles à l'investigation

Remarque : En plus d'être indispensable à la compréhension de l'incident, sauvegarder les éléments de preuve pourra être nécessaire pour répondre aux forces de l'ordre lors d'éventuelles poursuites judiciaires.

Actions d'endiguement par thèmes

Limiter l'extension de la compromission

Mesure 6 - Limiter la propagation depuis la messagerie compromise

Action 6.a : Vérifier les courriels du compte compromis

- ❑ Détection de courriels frauduleux envoyés vers d'autres cibles, externes ou internes
- ❑ Détection de courriels frauduleux supprimés dans la corbeille
- ❑ Détection de courriels indiquant des réinitialisations de mot de passe ou d'appareils de confiance
- ❑ Détection de courriels contenant des identifiants (mots de passe, clés SSH, QR Code, etc.), qui seront tous à considérer compromis car potentiellement accédés par l'attaquant
- ❑ Détection de règles de suppression et lecture automatique de messages reçus (utilisée pour cacher les retours de mail de personnes contactées durant l'usurpation)

Remarque : Si vous avez détecté une adresse IP suspecte, vous pouvez directement identifier les actions commises par l'adresse dans les journaux et les analyser.

Action 6.b : Vérifier les fichiers sensibles accessibles du compte compromis

- ❑ Détecter des fichiers sensibles dans la boîte de messagerie du compte compromis
- ❑ Détecter des fichiers sensibles auxquels peut accéder le compte via des partages de fichiers liés à la messagerie (exemple pour Microsoft 365 : SharePoint, Teams, etc.)
    - Vérifier dans les journaux si l'attaquant a effectivement accédé à ces fichiers sensibles

Mesure 7 - Entraver l'attaquant

Action 7.a : Mettre en détection les adresses IP identifiées

- ❑ Identifier les adresses IP sources avec lesquelles le compte a été illégitimement accédé
- ❑ Mettre en détection ces adresses IP sources, pour pouvoir voir quels autres comptes l'attaquant a obtenu, et avec lesquels il tente de se connecter
    - Il sera plus efficace de mettre ces adresses IP en détection plutôt que de les bloquer, car cela donnera plus d'informations sur l'étendue de la compromission
    - Mettre en détection ces adresses IP sources, pour pouvoir voir quels autres comptes l'attaquant a obtenu, et avec lesquels il tente de se connecter

Remarque : Certains attaquants sont en capacité de changer fréquemment d'adresse IP. Si l'attaquant dispose d'une persistance sur la messagerie, le blocage de l'adresse IP n'aurait donc pas d'impact.

Actions d'endiguement par thèmes

Limiter l'extension de la compromission

Mesure 7 - Entraver l'attaquant

Action 7.b : Investiguer l'accès initial

- ❑ **Phishing** : Investiguer des **courriels suspects** pouvant donner lieu à une compromission (URL de phishing, ...)
- ❑ **Infostealer** : Investiguer les **pièces jointes suspectes** pouvant donner lieu à une compromission (logiciel malveillant, ...)

Action 7.c : Bloquer toute tentative d'accès initial

Si l'accès initial de la compromission a pu être identifié précédemment :

- ❑ Mettre en quarantaine ou bloquer les messages entrants de l'expéditeur ou de tout le domaine source de messagerie malveillant
- ❑ Bloquer les mails entrants contenant des indicateurs identifiés (IP, URL, pièces jointes, ...)
- ❑ Bloquer les requêtes web vers l'URL identifiée malveillante
- ❑ Bloquer des types de fichiers identifiés (exécutable, archive avec un mot de passe, etc.)

De plus, si l'origine de la compromission est un tiers de confiance :

- ❑ Contacter le tiers de confiance pour l'alerter de la probable compromission du compte expéditeur

Impacts : Bloquer un domaine source, surtout s'il est de confiance, peut avoir des effets importants sur l'activité et la relation avec le tiers. Il est nécessaire d'anticiper les conséquences de cette action et de prévenir le service d'assistance HelpDesk. Cet impact peut être relativisé si votre solution de messagerie propose des blocages temporaires des indicateurs (par exemple, blocage de l'expéditeur pendant 7 jours).

Sur l'application de messagerie (si cela possible), à la place de bloquer l'adresse IP, il est possible de la placer en détection/supervision afin de pouvoir identifier quels autres comptes l'attaquant a obtenus et avec lesquels il tente de se connecter.

Actions d'endiguement par thèmes

Débuter l'investigation

Mesure 8 - Investiguer le système d'information

Remarque : Cette mesure va au-delà d'un endiguement classique et doit être considérée comme des actions propres à un début d'investigation plus poussée.

Action 8.a : Détecter les événements inhabituels liés à la messagerie

- ❑ Détecter des connexions provenant de localisations, de systèmes inhabituels sur le compte compromis et/ou d'autres comptes ou systèmes
- ❑ Détecter des connexions provenant d'équipements de connexion inhabituels sur le compte compromis et/ou d'autres comptes ou systèmes
- ❑ Détecter des connexions d'adresses IP inhabituelles sur le compte compromis et/ou d'autres comptes ou systèmes
- ❑ Détecter des connexions à des horaires inhabituels sur le compte compromis et/ou d'autres comptes ou systèmes
- ❑ Détecter des alertes d'échecs de connexion suivies d'une connexion réussie suspecte sur le compte compromis et/ou d'autres comptes ou systèmes
- ❑ Détecter des erreurs **MFA** sur le compte compromis et/ou d'autres comptes ou systèmes
- ❑ Détecter des notifications de voyage impossible

Action 8.b : Détecter les événements inhabituels en dehors de la messagerie

- ❑ Détecter des connexions vers des IP/domaines rares, ou tout autre flux inhabituel
- ❑ Détecter des actions anormales sur le système d'information réalisées avec le compte de l'utilisateur victime

Actions d'endiguement par thèmes

Débuter l'investigation

Mesure 8 - Investiguer le système d'information

Action 8.c : Détecter des anomalies sur le poste utilisateur

- ❑ Si le login/mot de passe a été extrait par du *phishing*, inutile de suspecter une compromission du poste utilisateur
- ❑ Si aucun élément ne permet de connaître la méthode de récupération du login/mot de passe, investiguer la présence d'un *infostealer* sur le poste utilisateur en commençant par les alertes antivirales ou de l'EDR
- ❑ Si une alerte a détecté un *infostealer*, superviser si d'autres postes ont eu la même alerte

En fonction des détections opérées pendant cette phase, il conviendra de récupérer les indicateurs afin d'orienter les recherches sur d'autres comptes/postes potentiellement compromis et de déterminer le périmètre réel de la compromission.

*Si, lors de cette phase, une compromission étendue sur le système est détectée ou suspectée, il est possible de se référer à la fiche dédiée : Fiche Réflexe - Compromission système – Qualification (*https://cyberveille.esante.gouv.fr/dossier-thematique/compromission-systeme-qualification-et-endiguement*)*

Actions d'endiguement par thèmes

Sécuriser l'organisation

Mesure 9 - Préserver les traces

Remarque : Cette partie comprend des mesures structurelles à appliquer au sein de votre organisation pour la sécuriser sur le long terme.

Action 9.a : Sécuriser les mots de passe

- ❑ Configurer une politique de mots de passe **forts**, et surtout **longs**
- ❑ Configurer des mesures permettant d'empêcher les attaques par *force brute* sur l'authentification

Action 9.b : Réinitialiser les autres comptes

- ❑ Forcer le renouvellement de **mot de passe** et du **MFA**. Si plusieurs comptes ont été compromis dans la même période, le faire pour tous les utilisateurs.

Action 9.c : Généraliser l'usage du MFA

- ❑ Imposer l'usage du **MFA** pour les comptes administrateurs, sans exception
- ❑ Tendre à imposer l'usage du **MFA** pour tous les comptes sensibles
- ❑ Généraliser le **MFA** à tous les utilisateurs, seule mesure générale vraiment efficace contre l'usurpation de compte

Action 9.d : Sécuriser la solution de messagerie

- ❑ Vérifier si la solution de messagerie est à jour, et si besoin la **mettre à jour**
- ❑ Vérifier si la solution de messagerie est affectée par une vulnérabilité, et suivre les recommandations de l'éditeur et la sortie d'un **correctif de sécurité**

Actions d'endiguement par thèmes

Sécuriser l'organisation

Mesure 10 – Sensibiliser l'utilisateur

Action 10.a : Sensibiliser l'utilisateur

- ❑ Sensibiliser l'utilisateur à ne pas utiliser le même mot de passe sur les différentes applications de l'organisation et à différencier ses mots de passe des environnements professionnels et personnels
- ❑ Sensibiliser l'utilisateur sur les responsabilités et les risques d'une usurpation d'identité via une boîte mail

Suite des actions

A la fin de ces actions d'endiguement, la compromission devrait être contenue. Cela étant, seule une analyse approfondie permettra d'appréhender les indicateurs décelés durant cette première phase de remédiation.

De manière générale, un incident doit être géré jusqu'à son terme avec tous les corps de métier concernés : **investigation forensique et remédiation par une équipe spécialisée**, **maintien d'activité**, **communication interne aux partenaires**, **dépôt de plainte et déclarations**, etc.

Pour ce faire, il est conseillé de piloter la suite de la résolution de l'incident en cohérence avec les impacts identifiés et demander de l'aide :

- Mettre en œuvre une **gestion d'incident cyber** pour piloter la résolution de l'incident.
  Voir les annexes Contacts et Déclarations

Remarque :

- Si vous vous apercevez que votre organisation a été susceptible de transmettre des courriels frauduleux à des tiers, il conviendra de les prévenir. Aussi, il serait judicieux de vérifier que l'organisation ne fait pas l'objet d'un blocage auprès de ces tiers (par exemple en vérifiant les logs des mails sortants vers ces tiers).
- Si la source du message suspect est un tiers ou un partenaire de confiance, il peut être raisonnable d'en informer l'entreprise concernée.
- Si une adresse mail identifiée comme du spam a été détectée lors de l'investigation, il est possible de la signaler auprès de Signal Spam (https://www.signal-spam.fr)
- Enfin, en cas de campagne étendue de **phishing** ou de **spam** à destination de votre organisation, il est conseillé de réaliser une communication auprès des utilisateurs afin de les sensibiliser, de leur rappeler les bonnes pratiques, et éventuellement de relater de manière transparente l'incident.

Annexes

Définitions

Compromission d'un compte de messagerie

Une **compromission d'un compte de messagerie** désigne un accès non autorisé à un compte de messagerie, par un attaquant. Ce dernier peut alors lire et envoyer des courriels à l'insu de l'utilisateur légitime du compte, et accéder à ses données.

Qualifier un incident

Qualifier un incident signifie :

- **Confirmer** qu'un incident de sécurité est bien en cours et si oui, déterminer précisément sa *nature*.
- **Évaluer la gravité/priorité de l'incident** en évaluant le *périmètre* affecté, l'*impact* potentiel sur le fonctionnement de l'organisation et l'*urgence* à le résoudre.

La qualification permettra de prendre des décisions éclairées sur la réponse à l'incident et d'allouer les ressources appropriées pour le résoudre.

Endiguer un incident

L'endiguement désigne l'ensemble des actions prises au début d'un incident de sécurité informatique destinées à en contenir l'ampleur. Elles n'ont généralement pas vocation à être prolongées durablement.

Axes d'évaluation

- **Périmètre** : Le périmètre d'un incident désigne son étendue sur les composants du système d'information (comptes, applications, systèmes, etc..) et leur administration.
- **Impact** : L'impact d'un incident désigne le niveau de perturbation et de dommage potentiel qu'il engendre pour l'organisation.
- **Urgence** : L'urgence d'un incident désigne la rapidité avec laquelle il faut réagir pour rétablir les activités essentielles impactées.

Degrés de gravité

- **Anomalie courante** (gravité **faible**) : Une anomalie courante est un incident de sécurité ne représentant pour l'instant pas de menace sérieuse pour la sécurité du système d'information et n'entraînant pas d'impact significatif sur l'activité métier. Elle nécessite tout de même d'être correctement qualifiée pour confirmer son faible degré de gravité.
- **Incident mineur** (gravité **modérée**) : Un incident mineur est un incident de sécurité représentant une menace limitée pour le système d'information et entraînant - ou risquant d'entraîner - un impact modéré sur l'activité métier.
- **Incident majeur** (gravité **élevée**) : Un incident majeur est un incident de sécurité représentant une menace sérieuse pour le système d'information et entraînant - ou risquant d'entraîner - un impact fort sur l'activité métier.
- **Crise cyber** (gravité **critique**) : Une crise cyber représente un incident de sécurité ayant un *périmètre étendu* sur le système d'information, un *impact fort* sur l'activité métier et nécessitant une *résolution urgente*.

Annexes

Contacts

La gestion d'un incident cyber implique de faire appel à des équipes spécialisées au sein de CERT/CSIRT, qui appuieront les équipes internes dans la réalisation de leurs actions de défense.

Qui ?	Comment ?	Pour qui ?
CERT/CSIRT interne de l'organisation		
CERT Santé	https://esante.gouv.fr/produits-services/cert-sante https://cyberveille.esante.gouv.fr/	Pour les organisations du secteur de la santé et du médico-social
CERT/CSIRT externe en prestation de réponse à incident	https://www.cybermalveillance.gouv.fr/diagnostic/accueil https://cyber.gouv.fr/produits-services-qualifies	Pour les petites organisations : consulter le registre des prestataires spécialisés sur Cybermalveillance Pour les organisations opérant un système d'information complexe : faire appel à un Prestataire qualifié de Réponse à Incidents de Sécurité (PRIS)
CERT-FR	https://www.cert.ssi.gouv.fr/contact	Pour les administrations et les Opérateurs d'importance vitale et de services essentiels
CSIRT régional	https://www.cert.ssi.gouv.fr/csirt/csirt-regionaux	Pour les organisations de taille intermédiaire : collectivités territoriales, PME, ETI ou associations

De plus, pour les incidents complexes, une aide externe est également recommandée pour :

- Gérer la crise
- Gérer la communication interne et externe
- Augmenter les ressources humaines et capacitaires de reconstruction de votre direction informatique

Pour faciliter la mobilisation de tous ces acteurs, il est conseillé de s'appuyer sur des annuaires tenus à jour en amont et accessibles même en cas d'indisponibilité du système d'information.

Annexes

Déclarations complémentaires

Conjointement à la résolution de l'incident, des déclarations doivent être effectuées :

Qui ?	Comment ?	Pourquoi ?
ANSSI	https://www.cert.ssi.gouv.fr/contact/ https://cyber.gouv.fr/notifications-reglementaires	L'administration, les opérateurs d'importance vitale et de services essentiels, et toute organisation impliquant des informations classifiées, doivent déclarer leurs incidents à l'ANSSI.
Dépôt de plainte	https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/comment-porter-plainte-en-cas-de	Déposer plainte permet de déclencher une enquête et de dégager votre responsabilité en cas de propagation de l'attaque à d'autres victimes.
CNIL	https://www.cnil.fr/fr/notifier-une-violation-dedonnees-personnelles	Les incidents affectant des données personnelles doivent faire l'objet de déclaration à la CNIL dans un délai de 72 heures. En cas de doute, il faut faire une pré-déclaration précisant avoir subi une potentielle compromission même si aucune exfiltration de données n'a été confirmée.
Autres autorités		Une organisation d'un domaine réglementé (finance, santé, etc.) est astreinte à des obligations de déclaration spécifiques. Dans le doute, consulter le service juridique.

Annexes

Préparation

En **prévention** d'un incident, une fiche réflexe sera d'autant plus efficace si elle a pu être contextualisée et traduite en une **procédure interne et actionnable immédiatement** à son système d'information. Dans une situation d'urgence, elle augmentera la rapidité de la réponse, minimisera les erreurs de manipulation et permettra à une personne d'astreinte moins expérimentée de mener ces actions.

Préparation

Lors d'une lecture préparatoire de cette fiche ou pour aller plus loin dans la compréhension et la mise en œuvre des notions évoquées, certains documents annexes peuvent être utiles :

- Fiche réflexe - Compromission d'un compte de messagerie - Qualification (https://cyberveille.esante.gouv.fr/dossier-thematique/compromission-systeme-qualification-et-endiguement)
- Fiches techniques du CERT Santé pour améliorer la sécurité de son SI (https://cyberveille.esante.gouv.fr/se-proteger-contre-les-menaces)
- Fiches reflexes du CERT Santé pour réagir à un acte de cyber malveillance (https://cyberveille.esante.gouv.fr/reagir-un-acte-de-cybermalveillance)
- Comment réagir en cas d'incident rançongiciel (https://cyber.gouv.fr/publications/attaques-par-rancongiciels-tous-concernes)
- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique (https://cyber.gouv.fr/publications/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique)
- Cyberattaques et remédiation (https://cyber.gouv.fr/piloter-la-remediation-dun-incident-cyber)

Annexes

Licence

Ce document est dérivé des travaux du GT Fiches Réflexes de remédiation de l'InterCERT France

Les documents originaux peuvent être consultés sur le site de l'InterCERT-France (https://www.intercert-france.fr/).